



COPY OF PAPERS  
ORIGINALLY FILED

### ABSTRACT

A method for digitally signing a message is described. The method includes providing a message digest ( $M_x, M_z$ ), providing a modulus  $N$ , providing a number  $V$  in a ring  $Z_N$ , wherein for another number  $S$  in the ring  $Z_N$ ,  $V \cdot S^2 = 1$  in  $Z_N$ , solving the equation  $(M_x + x)^2 - V \cdot y^2 = 4 \cdot (M_z + z)$  in  $Z_N$  to produce  $x$ ,  $y$ , and  $z$ , and assigning SIG as the signature of  $(M_x, M_z)$ , wherein SIG includes  $(x, y)$ . Related methods and apparatus are also described.

20020404-03500